Hillstone W-Series

Firewall WAF (Web Application Firewall)

Rozwiązanie Hillstone W-Series WAF (Web Application Firewall) zapewnia kompleksowe bezpieczeństwo klasy korporacyjnej dla webowych serwerów, aplikacji i API. Chroni przed atakami zarówno na warstwie sieci jak i aplikacji, zabezpieczając przed atakami DDoS, 10 głównymi zagrożeniami z zestawienia OWASP oraz atakami z wykorzystaniem botów, itp. Ponadto, WAF weryfikuje interfejsy API ze schematem określonym w OpenAPI i automatycznie generuje odpowiednie polityki do wykrywania i obrony przed takimi atakami i niepożądanym wykorzystywaniem API.

Hillstone WAF łączy tradycyjne, oparte na regułach wykrywanie zagrożeń z innowacyjną analizą semantyczną. Takie podejście istotnie zwiększa dokładność, a jednocześnie minimalizuje liczbę fałszywych alarmów. Rozwiązanie Hillstone WAF wykorzystuje także technologię uczenia maszynowego, aby odpowiednio dostosowywać polityki bezpieczeństwa oraz blokować nieznane zagrożenia i ataki. Co więcej, wielowymiarowe logi mogą być automatycznie agregowane, aby administratorzy mogli łatwo identyfikować anomalie lub lokalizować fałszywe alarmy, a następnie w razie potrzeby udoskonalać dotychczasowe polityki.

Najważniejsze cechy produktu

Pełne bezpieczeństwo aplikacji webowych

Rozwiązanie Hillstone WAF (Web Application Firewall) zapewnia pełną ochronę aplikacji webowych i API dla przedsiębiorstw i innych organizacji. Wykrywa i zabezpiecza przed atakami zarówno na warstwie sieciowej (np. ataki DDoS, flooding, scanning, spoofing, itp.) jak i aplikacji (np. 10 głównych zagrożeń z zestawienia OWASP, w tym wstrzykiwanie kodu, XSS - cross site scripting, itp.). Hillstone WAF automatycznie wykrywa serwery web i powiązane z nimi zasoby, a następnie odpowiednio je chroni. Tym samym, Hillstone WAF zabezpiecza całe środowisko sieci web, nawet jeżeli podlega ono skalowaniu, co pomaga poprawić efektywność operacyjną i szybciej dostarczać rezultaty biznesowe.

Zaawansowana ochrona API

Wraz z rozwojem projektów związanych z cyfrową transformacją, interfejsy API odgrywają coraz większą rolę w procesach rozwoju i integracji aplikacji. Popularność API sprawia, że stanowią one dodatkowy element wykorzystywany do przeprowadzenia ataków na sieć, ze względu na nadmierne eksponowanie danych, brak zasobów i ograniczenia pasma, ataki związane ze wstrzykiwaniem kodu lub XSS do komunikatów API, itp. Opierając się na schemacie zdefiniowanym przez OpenAPI, Hillstone WAF weryfikuje poprawność API i generuje polityki do wykrywania ewentualnych zagrożeń.

Wyższa dokładność i skuteczność detekcji, dzięki zastosowaniu dwóch mechanizmów analitycznych

Hillstone WAF integruje najbardziej innowacyjną na rynku analizę semantyczną z tradycyjnym mechanizmem wykrywania zagrożeń. Dzięki połączeniu z tradycyjnym, opartym na rolach wykrywaniu zagrożeń, mechanizm analiz semantycznych pozwala skuteczniej wykrywać zagrożenia takie jak wstrzykiwanie SQL czy XSS, a jednocześnie minimalizuje liczbę fałszywych alarmów. Funkcja dekodowania rekurencyjnego Hillstone WAF pozwala wykrywać ataki, które są niewidoczne ze względu na zastosowanie wielu warstw kodowania. Takie podejście istotnie poprawia dokładność i skuteczność wykrywania zagrożeń.

Optymalizacja reguł bezpieczeństwa z użyciem uczenia maszynowego i obrona przed nieznanymi atakami

Oprócz ogólnej ochrony opartej na regułach i skryptach dotyczących znanych ataków, funkcja automatycznego uczenia się dostępna w Hillstone WAF pozwala ograniczać wpływ nieznanych zagrożeń, w celu ochrony określonych aplikacji przed atakami typu zero-day. Model wykorzystujący uczenie maszynowe uczy się normalnego ruchu sieciowego (np. długość parametrów, ciasteczka, metody HTTP) i dostosowuje się do wyników testów oraz informacji przekazywanych przez administratorów. Jest to proces ciągły, polegający na aktualizacji i optymalizacji reguł WAF wraz z rozwojem aplikacji. W ten sposób istotnie ograniczane są wysiłki operacyjne, dzięki eliminacji konieczności analizy fałszywych alarmów oraz ręcznego dostosowywania polityk bezpieczeństwa.

Rozbudowane logi dla inteligentnej analizy i raportów

Hillstone WAF zapewnia administratorom i operatorom sieci wysoki poziom widoczności i kompleksowe raporty wraz z analizą zagrożeń, ruchu, ataków i kontrolą środowiska. Funkcja agregacji logów, łączy informacje z wielu źródeł, co pozwala na łatwe identyfikowanie podejrzanych zachowań i fałszywych alarmów, a następnie odpowiednie konfigurowanie polityk.

Cechy

Ochrona aplikacji webowych

- Obrona przed anomaliami HTTP
- Transparentne proxy SSL
- Obrona przed atakami HTTP fast flood i slow flood
- Obrona przed atakami związanymi z wstrzykiwaniem SQL, LDAP, SSI, Xpath, komend, RFI (Remote File Include), itp.
- Ochrona przed atakami cross-site, w tym XSS i CSRF
- Wykrywanie wstrzykiwania SQL i ataków XSS z wykorzystaniem analizy semantycznej
- Ochrona przed wyciekiem danych, w tym błędów serwera i bazy danych, treści katalogu sieci Web, kodu, słów kluczowych, itp.
- Ochrona przed wyciekiem wrażliwych danych osobowych, np. numerów identyfikacyjnych, numerów kart bankomatowych i kredytowych, kont mailowych. Obsługuje odkodowywanie wrażliwych danych (zastępowanie specjalnych znaków)
- Bezpieczeństwo plików cookie. Ochrona przed manipulacją i przejmowaniem takich plików. Obsługa sygnatur i szyfrowania plików cookie.
- Funkcja kontroli dostępu do sieci web, tj, ochrona przed skanowaniem, crawlingiem, przekierowaniem katalogów
- Szczegółowa kontrola dostępu HTTP w oparciu o adres IP klienta, metodę, nagłówek, zawartość, wersję protokołu HTTP, ścieżkę URI, itp.
- Obrona przed atakami na luki bezpieczeństwa serwerów web infrastruktury web i aplikacji webowych
- Obrona przed nielegalnym dostępem do zasobów, w tym wgrywaniem i pobieraniem plików, linkowaniami. Kontrola procesu pobierania opiera się na rozmiarze pliku i typie pliku MIME.
- Obrona przed złośliwym oprogramowaniem, w tym ataki WebShell i konie trojańskie
- Obrona przed atakami brute force
- Możliwość wykrywania i blokowania klientów wg ich źródłowego adresu IP (X-forward-for), przy wdrożeniu za proxy lub load balancerem
- Obsługa reguł tworzonych przez użytkownika
- Predefiniowane szablony polityki bezpieczeństwa. Możliwość tworzenia własnych polityk
- Na bieżąco aktualizowana baza sygnatur
- Wykrywanie zagrożeń i ochrona API. Weryfikacja w oparciu o specyfikację OpenAPI.
- Wykrywanie ruchu botów i funkcja anti-crawler w oparciu o sygnatury urządzeń, weryfikacja CAPTCHA pod względem podejrzanego ruchu, blokowanie ruchu na podstawie sygnatur urządzeń
- Obsługa konfiguracji stanu lokalizacji, w ramach utrzymania strony internetowej
- Wsadowa konfiguracja lokalizacji

Ochrona przed zniekształcaniem informacji

- 2 tryby pracy: tryb uczenia się i tryb ochrony
- Porównywanie podobieństw chronionych zasobów
- Obsługa własnych typów chronionych, statycznych stron internetowych. Obsługa listy wyjątków URL dla zapewnienia odpowiedniego bezpieczeństwa. Możliwość określenia czasu trwania ochrony
- Synchronizacja z serwerami i ustalenia stanu bazowego w ramach wbudowanego mechanizmu synchronizacji
- Monitorowanie modyfikacji konfiguracji
- Zbieranie informacji dochodzeniowych o modyfikacjach

Ochrona bezpieczeństwa sieci

- Obsługa Virtual Patching w oparciu o wyniki skanowania podatności lub zaimportowane raporty
- Obrona przed atakami DoS, w tym ping of death, Teardrop, fragmentacja IP, Smurf&Fraggle, Land, ICMP, itp.
- Ochrona przed atakami DNS query flooding, możliwość konfiguracji poziomu powiadamiania w oparciu o adres źródłowy i docelowy
- Ochrona przed anomaliami TCP
- Ochrona przed skanowaniem/ spoofingiem adresu IP i skanowaniem portu
- Obrona przed floodingiem, np. ICMP, UDP, SYN, itp.
- Obsługa funkcji reputacji adresów IP i blokowania złośliwych adresów IP
- Kontrola polityk w oparciu o nagłówek HTTP, w tym host, user-agent, Accept, Accept-LAN, Accept-Encoding, Referer, pliki Cookie, itp.
- Obsługa HTTP2 w trybie reverse proxy
- Obsługa deszyfrowania HTTPS i wykrywania ruchu IPv6 w trybie TAP

IPv6

- Optymalizacja polityk kontroli dostępu
- Obsługa podwójnego stosu protokołów IPv4 i IPv6. Adresy IPv4 i IPv6 mogą być jednocześnie dodawane jako chronione

Automatyczne uczenie się polityk

- Wykrywanie i ochrona ruchu IPv6
- Inteligentne uczenie się ruchu w chronionych lokalizacjach i dostosowywanie polityk do wyników nauki
- Elementy podlegające nauce: dynamiczny adres URL, parametr URL, metoda dostępu HTTP, pliki cookie i inne informacje
- Obsługa trybu uczenia się i tryby ochrony. Możliwość automatycznego przełączenia na tryb ochrony po zakończeniu nauki

Działania obronne

- Uczenie się z określonego URL
- Alarmowanie tylko jeżeli wykryte zostanie określone zachowanie

- Blokowanie zachowań, które łamią reguły bezpieczeństwa i reagowanie z wykorzystaniem specjalnej strony
- Możliwość dostosowania wyglądu strony z powiadomieniami
- Możliwość przekierowania strony z powiadomieniami na inny adres URL
- Możliwość tworzenia białych list (wyjątków) w oparciu o logi zabezpieczeń, adres URL, źródłowy adres IP
- Możliwość umieszczania atakujących na czarnej liście, w celu uniemożliwienia kolejnego dostępu do usługi
- Białe listy adresów IP i URL
- Współpraca z firewallem w celu tworzenia czarnych list
- Kontrola dostępu w oparciu o geolokalizację adresu IP

Wdrożenie

- Obsługa wielu trybów wdrożenia, w tym Transparent Proxy, TAP, Reverse Proxy, One-arm Reverse Proxy i Traction
- Automatyczne odkrywanie zasobów webowych
- Obsługa domyślnej lokalizacji
- Możliwość konfiguracji non-interface IP dla danej lokalizacji oraz odpowiedzi ARP w trybie One-arm Reverse Proxy i Reverse Proxy
- Graficzny kreator wdrożenia

Wsparcie wirtualizacji

- Obsługiwane hypervisory: VMware, KVM, Openstack i Xen
- Obsługa wbudowanego agenta, np. VMware Tools i Cloud-init
- Obsługa AWS, Azur, AliCloud
- Obsługa wdrożenia o wysokiej dostępności w środowisku chmury publicznej (AliCloud, AWS)
- Zarządzanie licencjami przez system LMS
- Obsługa API RESTful
- Obsługa kart rozszerzeń NIC typu hot-swap SR-IOV i elastycznego skalowania

Wysoka dostępność

- Tryb aktywny / pasywny
- Tryb Active/ Active Peer
- Obsługa programowego bypassu (w trybie transparent proxy)

Przyspieszenie aplikacji i równoważenie obciążenia serwera

- Obsługa cache stron web, kompresowania stron i Multipleksacji TCP, SSL unloading, SSL proxy
- Sprzętowe przyspieszenie SSL
- Obsługa równoważenia obciążenia serwera (w trybie Reverse Proxy), w tym algorytmy WRR, Least Connection i IP Hash
- Równoważnie obciążenia serwera w sieciach IPv6
- Sprawdzanie stanu serwera. Możliwość dostosowania obiektu URL na potrzeby sprawdzania stanu.
- Wykorzystywanie nagłówka X-header jako równoważenia obciążenia IP

Konfiguracja sieci i interfejsów

- Obsługa statycznego routingu
- Obsługa agregacji interfejsów
- Obsługa sub-interfejsu VLAN
- Obsługa wielu vSwitch, virtual-wire
- Obsługa LLDP

Uwierzytelnianie

- Wielopoziomowa autoryzacja, predefiniowane role, w tym administratorzy systemu, operatorzy, audytorzy, itp.
- Obsługa lokalnego uwierzytelniania, RADIUS i TACAS-C+

Zarządzanie urządzeniami

- Wiele metod zarządzania, w tym: HTTP, HTTPS, SSH, konsola, itp. Możliwość konfiguracji zaufanego hosta zarządzającego
- Monitorowanie stanu urządzenia, w tym: ogólne i szczegółowe informacje o wykorzystaniu i temperaturze dysku, pamięci i CPU
- Scentralizowane zarządzanie i aktualizowanie firmware poprzez HSM (Hillstone Security Management System)
- Obsługa narzędzi do obsługi i utrzymania takich jak ping/tcpdump/curl

Logi, raporty i alarmy

- Bogate informacje o logach, w tym logi dotyczące zarządzania urządzeniami, bezpieczeństwa sieci, bezpieczeństwa stron web, zabezpieczeń, kontroli dostępu, strategii automatycznego uczenia się, dostępu do stron web, itp.
- Rejestrowanie wszystkich nagłówków HTTP podczas ataków, w tym URL, User-Agent, zawartość POST, pliki cookie itp.
- Rejestrowanie odpowiedzi serwera
- Powiadamianie poprzez e-mail, SNMP, SYSLOG, SMS, itp.
- Wielowymiarowe raportowanie, w tym przegląd zagrożeń bezpieczeństwa, szczegóły zagrożeń dla lokalizacji, informacje o typie ataku, analiza zmian lokalizacji, liczba odwiedzin, podsumowanie ataku na warstwę sieci, stan systemu operacyjnego, itp.
- Agregacja logów według polityki lub IP klienta
- Inteligentna analiza logów, w tym analiza zagrożeń i fałszywych alarmów oraz optymalizacja polityki bezpieczeństwa w oparciu o wyniki analiz
- Odtwarzanie ataku na potrzeby analizy i lokalizowania zagrożeń i ataków w sieci
- Możliwość ręcznego badania podejrzanych alertów i raportowanie fałszywych alarmów do CloudView
- Możliwość usunięcia logów bezpieczeństwa web
- Przesyłanie logów przez FTP
- Tworzenie własnych raportów przez użytkownika
- Eksport raportów do plików PDF, DOC
- Cykliczne eksportowanie raportów
- Serwer poczty obsługuje szyfrowaną transmisję STARTTLS i SSL
- Śledzenie sesji użytkownika w celu dodania do logów nazwy użytkownika, identyfikatora sesji oraz i parametru tożsamości sesji
- Możliwość wysyłania raportów poprzez FTP i email

Specyfikacja techniczna

	W120S	W320S	W620S	W1120S
				
Przepustowość HTTP	600 Mbps	1 Gb/s	1.5 Gb/s	3.5Gb/s
Liczba nowych sesji HTTP	1,600	3,500	5,000	8,000
Maks. transakcji HTTP na sekundę (TPS)	2400	5,500	7,000	10,000
Dysk	480G SSD	480G SSD	480G SSD	480G SSD
Pamięć RAM	4G	4G	8G	16G
Porty zarządzania	2 x USB, 1 x port zarządzania, 1 x port konsoli	2 x USB, 1 x port zarządzania, 1 x port konsoli	2 x USB, 1 x port zarządzania, 1 x port konsoli, 1 x port HA (SPF)	2 x USB, 1 x port zarządzania, 1x port konsoli, 1 x port HA (SPF)
Wbudowane porty I/O	8 x GE (w tym 1 para bypass)	8 x GE (w tym 1 para bypass)	2 x SFP+, 8 x SFP, 16 x GE (w tym 2 pary bypass)	2 x SFP+, 8 x SFP, 16 x GE (w tym 2 pary bypass)
Dostępne gniazda na moduły rozszerzeń	N/A	N/A	N/A	1
Opcjonalne moduły rozszerzeń	N/A	N/A	N/A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Liczba chronionych lokalizacji	8	16	32	64
Chronione pary IP/PORT	64	64	128	512
Parametry zasilania	50W, pojedynczy AC (natywny), podwójny AC (opcja)	50W, pojedynczy AC (natywny), podwójny AC (opcja)	100W, pojedynczy AC (natywny), podwójny AC (opcja)	100W, podwójny AC
Zasilacz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Obudowa	1U	1U	1U	1U
Wymiary (szer. x głęb. x wys.)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)
Waga	14.3 lb (6.5 kg)	14.3 lb (6.5 kg)	20.7 lb (9.4 kg)	26 lb (11.8 kg)
Temp. operacyjna	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Wilgotność względna	10%-95% bez kondensacji	10%-95% bez kondensacji	10%-95% bez kondensacji	10%-95% bez kondensacji

	W1520S	W3320S	W5602S	W7320S
				
Przepustowość HTTP	4 Gb/s	5 Gb/s	7 Gb/s	13 Gb/s
Liczba nowych sesji HTTP	10,000	14,000	22,000	45,000
Maks. transakcji HTTP na sekundę (TPS)	15,000	22,000	33,500	70,000
Dysk	480G SSD	960G SSD	960G SSD	960G SSD
Pamięć RAM	16G	32G	32G	64G
Porty zarządzania	2 x USB, 1 x port zarządzania, 1 x port konsoli, 1 x port HA (SPF)	2 x USB, 1 x port zarządzania, 1x port konsoli, 2 x porty HA (SFP+)	2 x USB, 1 x port zarządzania, 1x port konsoli, 2 x porty HA (SFP+)	2 x USB, 1 x port zarządzania, 1 x port konsoli, 1 x port HA (SFP+)
Wbudowane porty I/O	2 x SFP+, 8 x SFP, 16 x GE (w tym 2 pary bypass)	6 x SFP+, 16 x SFP, 8 x GE (w tym 2 pary bypass)	6 x SFP+, 16 x SFP, 8 x GE (w tym 2 pary bypass)	2 x QSFP+, 16 x SFP+, 8 x GE (w tym 4 pary bypass)
Dostępne gniazda na moduły rozszerzeń	1	1	1	1
Opcjonalne moduły rozszerzeń	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Liczba chronionych lokalizacji	128	256	512	512
Chronione pary IP/PORT	512	1024	1024	4096
Parametry zasilania	100W, Dual AC	280W, Dual AC	280W, Dual AC	300W, Dual AC
Zasilacz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Obudowa	1U	1U	1U	1U
Wymiary (szer. x głęb. x wys.)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)
Waga	26 lb (11.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)
Temp. operacyjna	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Wilgotność względna	10%-95% bez kondensacji	10%-95% bez kondensacji	10%-95% bez kondensacji	10%-95% bez kondensacji

Specyfikacja techniczna

	SG-6000-WV02	SG-6000-WV04	SG-6000-WV08	SG-6000-WV12
Przepustowość HTTP	1.2 Gb/s	2.5 Gb/s	5.5 Gb/s	8 Gb/s
Liczba nowych sesji HTTP	2,800	5,800	14,000	20,000
Maks. transakcji HTTP na sekundę (TPS)	3,000	6,500	16,000	22,000
Obsługa vCPU	2 rdzeniowy	4 rdzeniowy	8 rdzeniowy	12 rdzeniowy
Dysk (Min./Maks.)	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB
Pamięć RAM	4 GB	8 GB	16 G	24 G
Maks. liczba obsługiwanych interfejsów sieciowych	10	10	10	10
Chronione lokalizacje	16	32	128	256
Chronione pary IP/PORT	32	64	1024	1024

Dostępne moduły rozszerzeń

				
Module	IOC-W-4SFP+-A	IOC-W-2QSFP+-A	IOC-W-2MM-BE-A	IOC-W-2SM-BE-A
I/O Ports	4 x SFP+	2 x QSFP+	MM Bypass (2 pary portów bypass)	SM Bypass (2 pary portów bypass)
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)

UWAGA:
Wydajność ochrony HTTP określona przy skonfigurowanej chronionej lokalizacji i zastosowaniu strategii średniej ochrony